01-27-00

A

jc710 U.S. PTO
01/24/00

Practitioner's Docket No. 5010/097

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

jc511 U.S. PTO
09/489864
01/24/00

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Allan L. Samson; Michael Keilty

For (title): SYSTEM FOR PREVENTING TAMPERING WITH A SIGNAL CONDITIONER REMOTE FROM A HOST SYSTEM

1. Type of Application

This transmittal is for an original (nonprovisional) application.

2. Papers Enclosed

A. Required for filing date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

12 Page(s) of Specification
9 Page(s) of Claims
5 Sheet(s) of Drawing(s)--Formal

B. Other Papers Enclosed

5 Page(s) of declaration and power of attorney
1 Page(s) of abstract

CERTIFICATION UNDER 37 C.F.R. SECTIONS 1.8(a) AND 1.10*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

37 C.F.R. Section 1.10*

[ ] deposited with the United States Postal Service in an envelope addressed to Box Patent Application, the Assistant Commissioner for Patents, Washington, D.C. 20231. as "Express Mail Post Office to Address" Mailing Label No. EL471264633US (**mandatory**)

Date: 24 Jan 2000

William P. Wilbar

3. **Declaration or Oath**

Enclosed
Executed by: inventors.

4. **Inventorship Statement**

The inventorship for all the claims in this application is the same.

5. **Language**

English

6. **Assignment**

An assignment of the invention to Micro Motion, Inc. is attached. A separate "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" is also attached.

7. **Fee Calculation (37 C.F.R. Section 1.16)**
Regular Application

CLAIMS AS FILED

Claims	Number Filed	Basic Fee Allowance	Number Extra	Rate	Basic Fee 37 CFR 1.16(a) $690.00
Total Claims (37 CFR 1.16(c))	43	- 20 =	23 x	$18.00	$414.00
Independent Claims (37 CFR 1.16(b))	4	- 3 =	1 x	$78.00	$78.00
Multiple Dependent Claim(s), if any (37 CFR 1.16(d))			+	$260.00	$260.00

Filing Fee Calculation $1,442.00

8. Fee Payment Being Made at This Time

Enclosed	
Filing Fee	$1,442.00
Recording assignment ($40; 37 C.F.R. Section 1.21(h)) (See attached "COVER SHEET FOR ASSIGNMENT ACCOMPANYING NEW APPLICATION".)	$40.00
Total Fees Enclosed	$1,482.00

9. Method of Payment of Fees

Check in the amount of $1,482.00 is attached.

10. Authorization to Charge Additional Fees

The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 04-1697.

37 C.F.R. Section 1.16(a), (f) or (g) (filing fees)

37 C.F.R. Section 1.16(b), (c) or (d) (presentation of extra claims)

37 C.F.R. Section 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

37 C.F.R. Section 1.17(a)(1)-(5) (extension fees pursuant to SECTION 1.136(a))

37 C.F.R. Section 1.17 (application processing fees)

11. Instructions as to Overpayment

Credit Account No. 04-1697.

Date: 24 Jan 2000

William P. Wilbar
Registration No. 43,265
Duft, Graziano & Forest, P.C.
1790 30th Street, Suite 140
Boulder, CO 80301-1018
303-449-9497

SYSTEM FOR PREVENTING TAMPERING WITH A SIGNAL CONDITIONER REMOTE FROM A HOST SYSTEM

Field of the Invention

This invention relates to a signal processing system having a host system that provides power to and receives parameter signals from a signal conditioner that receives signals from sensors and generates the parameter signals. More particularly, this invention relates to a system that prevents tampering with the signal conditioner. Still more particularly, this invention relates to a tampering prevention system that is executed by the host system which periodically receives and stores authentication information from the signal conditioner.

Problem

It is common to buy and sell materials in measured quantities. For example, gas and oils are often sold in quantities of gallons or barrels. Therefore, it is critical that measurements of materials being delivered is accurate. In order to prevent fraud, government agencies require that devices measuring the amount of material being delivered are tamper proof. Some of these requirements are given in NIST Handbook 44 (1998 Edition) and OIML R 117 (1995 Edition).

One type of device used to measure material being delivered is a Coriolis Flowmeter. A Coriolis mass flowmeter measures mass flow and other information of materials flowing through a pipeline in the manner described by U.S. Patent No. 4,491,025 issued to J.E. Smith, et al. of January 1, 1985 and Re. 31,450 to J.E. Smith of February 11, 1982. A Coriolis mass flowmeter has one or more flow tubes of a curved or straight configuration. Each flow tube configuration in a Coriolis mass flowmeter has a set of natural vibration modes, which may be of a simple bending, torsional, radial, or coupled type. Each flow tube is driven to oscillate at resonance in one of these natural modes. The natural vibration modes of the vibrating, material filled systems are defined in part by the combined mass of the flow tubes and the material within the flow tubes. Material flows into the flowmeter from a connected pipeline on the inlet side of the flowmeter. The material is then directed through the flow tube or flow tubes and exits the flowmeter to a pipeline connected on the outlet side.

A driver applies a vibrational force to the flow tube. The force causes the flow tube to oscillate. When there is no material flowing through the flowmeter, all points

along a flow tube oscillate with an identical phase. As a material begins to flow through the flow tube, Coriolis accelerations cause each point along the flow tube to have a different phase with respect to other points along the flow tube. The phase on the inlet side of the flow tube lags the driver, while the phase on the outlet side leads the driver. Sensors are placed at two different points on the flow tube to produce sinusoidal signals representative of the motion of the flow tube at the two points. A phase difference of the two signals received from the sensors is calculated in units of time. The phase difference between the two sensor signals is proportional to the mass flow rate of the material flowing through the flow tube or flow tubes.

The sensors transmit the sinusoidal signals to a signal conditioner. The signal conditioner generates parameter signals that indicate properties of the material flowing through the flowmeter. The signal conditioner also generates a drive signal applied to the driver to vibrate the flow tubes. The parameter signals are then transmitted to a host system which provides the desired properties to a user.

In the past, manufacturers prevented tampering with the signal conditioner in the following manner. The signal conditioner has a security switch. The security switch prevents others from changing calibration information in the signal conditioner. Access to the security switch is prevented by placing the signal conditioner and host system in a housing which is sealed. In order to seal the housing, holes are drilled into opposing sides of the housing. A wire is then threaded through the housing and a lead seal is then placed on the wire. This allows for easy visual inspection to determine if the electronics have been tampered with.

However, the use of a seal on the housing is a problem for use in a sanitary operation. In a sanitary operation, the entire housing must be easily cleanable. An example of sanitary operations is the delivery of ingredients in a cooking system. In sanitary operation, the holes and seal have crevices and grooves that are hard to clean.

An alternative method of preventing tampering with the signal conditioner is to maintain an audit trail of changes in the signal conditioner. This allows for easy detection of tampering from a readout of the audit. However, the audit trail method requires a large amount of non-volatile memory and a real time clock. This adds greatly to the expense of each signal conditioner. Therefore, this is not a satisfactory solution for providing a tamper proof system.

Solution

The above and other problems are solved and an advance in the art is made by a tamper proof signal conditioner in accordance with this invention. A first advantage of the tamper proof signal conditioner in accordance with this invention is that the signal conditioner may be used in a sanitary environment. A second advantage is that the signal conditioner does not require additional memory or a real time clock in order to provide a tamper proof system.

In accordance with this invention, the signal conditioner and the host system are physically separated. The signal conditioner is circuitry that receives signals from sensors and converts the signals to parameter signals that indicate properties of a material. The host system supplies powers to the signal conditioner and receives the parameter signal from the signal conditioner. A conventional 4-wire cable connects the host system and signal conditioner to allow the host system to provide power to the signal conditioner and to transfer data between one another.

The host system is a processing unit that executes applications which provide the tamper proof system in accordance with this invention. The signal conditioner stores calibration and configuration data as well as a unique identification. For purposes of this invention, the signal conditioner may or may not contain a processing unit. For purposes of this discussion, the identification, calibration and configuration data are termed authentication data.

The host system periodically transmits a request to the signal conditioner for the authentication data. In a preferred embodiment, the host system and signal conditioner communicate using a Modbus™ protocol or HART™ protocol. The signal conditioner receives the request and reads the identification and calibration data. The identification and calibration data are then transmitted to the host system.

The host system stores the received information in a memory to provide an audit trail. The host system may also compare the received authentication information to initial information stored in the host system. If the authentication data does not match the initial information, the host system may generate an error signal. In response to the error signal, the host system may disable the system.

A first aspect of this invention is a system for preventing tampering with signal conditioning circuitry in electronics that determines a parameter from signals received from sensors and transmits the parameter to a host system. The host system

receives data from and send data to said signal conditioning circuitry and has a processing unit with a connected memory. Processing unit in the host system performs instructions stored in the memory that periodically transmit a request for authentication information to the signal conditioning circuitry, receive the authentication information the said signal conditioning circuitry, and store a record of the authentication information received from said signal conditioning circuitry in the memory.

A second aspect of the invention is that the authentication information includes a unique identification for the signal conditioning circuitry.

A third aspect of this invention is that the authentication information includes calibration data for the signal conditioning circuitry.

A fourth aspect of this invention is that the host system compares the authentication information with initial information, and signals an error in response to the authentication information not being equal to said initial information.

A fifth aspect of this invention is that the host system terminates operation of the system in response to the authentication information and initial information not being equal.

A sixth aspect of this invention is that the host system obtains the initial information.

A seventh aspect of this invention is that the host system obtains the initial information in the following manner. The host system transmits a initialize request to the signal conditioning circuitry for the authentication information in response to detecting a signal conditioning circuitry being connected to the host system. The host system then receives the authentication information from the signal conditioning circuitry and `stores the authentication information as the initial information in said memory.

An eighth aspect of this invention is that the host system compares the authentication information received from the signal conditioning circuitry with initial information and perform a programmed function in response to the authentication information not being equal to said initial information.

In a ninth aspect of this invention the signal conditioning circuitry includes a processing unit with a connected memory. The processing unit in the signal conditioning circuitry performs instructions to receive the request for the authentication

information the host system, to read the authentication information from the memory, and to transmit said authentication information to the host system.

In a tenth aspect of this invention, the record of the authentication information includes a time stamp indicating when the authentication information is received.

In an eleventh aspect of this invention the record includes the authentication information received from the signal conditioning circuitry.

Description of the Drawings

The above and other advantages of this invention are describe in the Detailed Description and the following drawings:

FIG. 1 illustrating a block diagram of a host system and a signal conditioner;

FIG. 2 illustrates an exemplary secondary processing system in a host system;

FIG. 3 illustrates a process executed by the host system in accordance with this invention;

FIG. 4 illustrating a process executed by the signal conditioner in accordance with this invention;

FIG. 5 illustrating a process executed by the host system to initialize the system in accordance with this invention; and

FIG. 6 illustrating a preferred embodiment of this invention in a Coriolis flowmeter.

Detailed Description

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which embodiments of the invention are shown. Those skilled in the art will appreciate that the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. In the drawings, like numbers refer to like elements throughout.

This invention relates to a system for preventing tampering with a signal conditioner. For purposes of this discussion, a signal conditioner is circuitry that receives signals from sensors and processes the signals to determine a system parameter. An example of a system parameter is a property of a material that the sensors are detecting. Those skilled in the art will recognize that the sensors may be attached to any type of device and that type of device is irrelevant to this invention.

In this system, the signal conditioner is enclosed in a housing that can be used in sanitary environments. This means the housing is easily cleaned. The signal conditioner is connected to a host system that is remote from the signal conditioner and in a separate housing. A host system and signal conditioner in accordance with this invention are shown below.

FIG. 1 illustrates a block diagram of a host system 100 and a signal conditioner 110 that incorporate the tamper proof system of this invention. Host system 100 includes a power supply 101 and a processing unit 102. Power supply 101 supplies the power needed to processing unit 102. Power supply 101 also supplies power to signal conditioner 110 via path 103. Processing unit 102 receives parameter signals from signal conditioner 110 and provides a parameter to user via path 26 and a secondary device. Processing unit 102 communicates with signal conditioner 110 via path 104 to receive the parameter signals and execute applications in accordance with this invention. In order to communicate, processing unit 102 and signal conditioner 110 may use any known protocol. Two exemplary protocols are HART™ and Modbus ™.

Signal conditioner 110 includes a sensor signal conditioner circuitry 112 and power converter 113. Sensor signal conditioner circuitry 112 receives sensor signals from sensors via path 114. The sensor signals are then converted by signal conditioner circuitry 112 into parameter signals. The parameter signals indicate a parameter of the system being measured by the sensors. One skilled in the art will recognize that sensor signal conditioner circuitry 112 may include a processing unit, such as a digital signal processor and the necessary circuitry needed to convert the sensor signals into digital signals that are readable by the processing unit. The parameter signals are then transmitted from signal conditioner circuitry 112 to host system 100 via path 104.

Power converter 113 receives power from host system 100. The power may then be converted and applied to the system being measured by the sensors or applied to the sensors. Power converter 113 also provides power to sensor signal conditioner circuitry 112 via path 116.

FIG. 2 illustrates an exemplary processing unit 200 which may be used as processing unit 102 in host system 100 or as a digital signal processor in signal conditioner 110 of FIG 1. Processing system 200 has a central processing unit (CPU)

201 which executes instructions read from a memory to perform applications that comprise the operations of processing system 200. One skilled in the art will recognize that CPU 201 may be a microprocessor, processor, or any combination grouping multiple processors and microprocessors. CPU 201 is connected to a memory bus 202. Memory bus 202 allows CPU 201 to access Read Only Memory (ROM) 203 and Random Access Memory 204. ROM 203 is a memory that stores instructions for performing the basic operative tasks of processing system 200. RAM 204 is a memory that stores the instructions and data needed to execute applications that are performed by processing system 200.

I/O bus 210 connects CPU 201 to a plurality of peripheral devices. CPU 201 receives and transmits data to the peripheral devices via I/O bus 210. The peripheral devices connected to I/O bus 210 include, but are not limited to, display 220, input device 230, network interface 240, and non-volatile memory 250. Display 220 is connected to I/O bus 210 by path 221 and includes a video driver and connected monitor for displaying information to a user. Input device 230 is connected to I/O bus 210 via path 231 and is a keyboard and/or mouse attached to an appropriate driver for receiving input data from a user. Network interface 240 is connected to I/O bus 210 via path 241 and may by a modem, Ethernet device driver, or other type of communications interface that allows processing system 200 to communicate with another device, such as a second processing system. Non-volatile memory 250 is a device, such as a disk drive, connected to I/O bus 210 via path 251 and which can read and write data to a disk or other storage media to store the data for future use. Peripheral device 260 is any other device that may be connect to I/O bus 210 via path 261 to share data with CPU 201.

FIG. 3 illustrates a process executed by processing unit 102 of host system 100 to provide a tamper proof system in accordance with the present invention. A tamper proof system in accordance with this invention stores a record of authentication data transmitted to the host system 100 from the signal conditioner 110 to ensure that someone does not tamper with signal conditioner 110. The authentication information is checked periodically to insure against tampering. Periodically means that the process may be executed at a set time interval, after a batch of a predetermined number of measurements are taken, or at random time intervals. The setting of the period is left to those skilled in the art.

Process 300 begins in step 301 with processing unit 102 in host system 100 transmitting a request for authentication information to signal conditioner 110. The authentication information may be a unique identification, calibration data, or other forms of data that does not change over time. It should be noted that combinations of these types of data may be used as well. Signal conditioner 110 receives the request and performs a process such as the one described below to transmit message containing authentication data back to processing unit 102 of host system 100.

In step 302, processing unit 102 receives the authentication information from the signal conditioner 110. A record of the received authentication information is then generated and stored in a memory in step 303. This provides an audit trail showing that there is no change in the signal conditioner 110.

After a record is stored, the received authentication information may be compared to initial information for the signal conditioner stored in the host system in step 304. This initial information may be received from the signal conditioner 110 at the time the system begins operation. Alternatively the initial information may be stored in a read only memory prior to operation to assure that the host system only operate with one pre-identified signal conditioner 110.

If the initial information matches the received authentication information then process 300 ends and waits to execute after the next period elapses. If the initial information does not match the received authentication information, the processing unit 102 may generate a signal indicating possible tampering or other type of error in step 306. The processing unit 102 may then cease operation of the system in step 307. The ceasing of operation prevents any potentially false reading from being used. Process 300 then ends.

FIG.4 illustrates an exemplary process 400 executed by a signal conditioner in response to receiving a request for authentication information. Process 400 begins in step 401 in which signal conditioner 110 receives the request from the host system. In response to receiving the request, signal conditioner 110 reads the authentication information from a memory. Preferably, the memory is a Read Only Memory to prevent tampering. Alternatively, if signal conditioner 110 contains a processing unit, signal conditioner 110 may generate the authentication information using a predetermined process executed by the processing unit that will generate an expected result. After the authentication information is retrieved, signal conditioner 110

generates a message including the authentication information and transmits the information to host system 100 in step 403 and process 400 ends.

Process 500 illustrated in FIG. 5 is an exemplary process executed by processing unit 102 in host system 102 to retrieve initial information to executed the processes in accordance with this invention. Process 500 begins in step 501 with processing unit 102 in host system 100 detecting a signal conditioner 110 connected to host system 100. Processing unit 102 transmits a request for authentication information to the signal conditioner 110 in step 502.

The signal conditioner receives the request and transmits authentication information for the signal conditioner 110 to host system 100. Processing unit 102 of host system 100 receives the authentication information in step 503. The authentication is then stored as initial information in step 504 and process 500 ends.

FIG. 6 illustrates one type of system that may use the tamper proof system in accordance with this invention. One skilled in the art will recognize the process in accordance with this invention may be applied to other types of systems to provide a tampering prevention system. FIG. 6 shows an exemplary Coriolis flowmeter 5 comprising a Coriolis flowmeter assembly 10 and meter electronics 20. Meter electronics 20 is connected to flowmeter assembly 10 via path 600 to provide density, mass flow rate, volume flow rate and totalized mass flow information over path 26. A Coriolis flowmeter structure is described although it should be apparent to those skilled in the art that the present invention could be practiced in conjunction with any apparatus having a vibrating conduit to measure properties of material flowing through the conduit. A second example of such an apparatus is a vibrating tube densitometer which does not have the additional measurement capability provided by a Coriolis mass flowmeters.

Meter assembly 10 includes a pair of flanges 601 and 601', manifold 602 and conduits 603A and 603B. Connected to conduits 603A and 603B are driver 604, pick-off sensors 605 and 605', and temperature sensor 607. Brace bars 606 and 606' serve to define the axis W and W' about which each conduit oscillates.

When Coriolis flowmeter 5 is inserted into a pipeline system (not shown) which carries the process material that is being measured, material enters flowmeter assembly 10 through flange 601, passes through manifold 602 where the material is directed to enter conduits 603A and 603B, flows through conduits 603A and 603B and

back into manifold 602 from where it exits meter assembly 10 through flange 601'.

Conduits 603A and 603B are selected and appropriately mounted to the manifold 602 so as to have substantially the same mass distribution, moments of inertia and elastic modules about bending axes W-W and W'-W', respectively. The conduits 603A-603B extend outwardly from the manifold in an essentially parallel fashion.

Conduits 603A-603B are driven by driver 604 in opposite directions about their respective bending axes W and W' and at what is termed the first out of phase bending mode of the flowmeter. Driver 604 may comprise any one of many well known arrangements, such as a magnet mounted to conduit 603A and an opposing coil mounted to conduit 603B and through which an alternating current is passed for vibrating both conduits. A suitable drive signal is applied by meter electronics 20 to driver 604 via path 610.

Pick-off sensors 605 and 605' are affixed to at least one of conduits 603A and 603B on opposing ends of the conduit to measure oscillation of the conduits. As the conduit 603A-603B vibrates, pick-off sensors 605-605' generate a first pick-off signal and a second pick-off signal. The first and second pick-off signals are applied to paths 611 and 611' prime. The driver velocity signal is applied to path 610.

Temperature sensor 607 is affixed to at least one conduit 603A and/or 603B. Temperature sensor 607 measures the temperature of the conduit in order to modify equations for the temperature of the system. Path 612 carries temperature signals from temperature sensor 107 to meter electronics 20.

Meter electronics 20 receives the first and second pick-off signals appearing on paths 611 and 611', respectively. Meter electronics 20 processes the first and second velocity signals to compute the mass flow rate, the density, or other property of the material passing through flowmeter assembly 10. This computed information is applied by meter electronics 20 over path 26 to a utilization means (not shown).

It is known to those skilled in the art that Coriolis flowmeter 5 is quite similar in structure to a vibrating tube densitometer. Vibrating tube densitometers also utilize a vibrating tube through which fluid flows or, in the case of a sample-type densitometer, within which fluid is held. Vibrating tube densitometers also employ a drive system for exciting the conduit to vibrate. Vibrating tube densitometers typically utilize only single feedback signal since a density measurement requires only the

measurement of frequency and a phase measurement is not necessary. The descriptions of the present invention herein apply equally to vibrating tube densitometers.

In this invention, the meter electronics 20 are physically divided into 2 components a host system 700 and a signal conditioner 701. In conventional meter electronics, these components are housed in one unit.

Signal conditioner 701 includes drive circuitry 710 and pick-off conditioning circuitry 720. One skilled in the art will recognize that in actuality drive circuitry 710 and pick-off conditioning circuitry 720 may be separate analog circuits or may be separate functions provided by a digital signal processor or other digital components. Drive circuitry 710 generates a drive signal and applies the drive signal to driver 604 via path 710 of path 600. In actuality, path 110 is a first and a second lead. Drive circuitry 710 is communicatively connected to pick-off signal conditioning circuitry 720 via path 713. Path 713 allows drive circuitry to monitor the incoming pick-off signals to adjust the drive signal. Power to operate drive circuitry 710 and pick-off signal conditioning circuitry 720 is supplied from host system 700 via a first wire 711 and a second wire 712. First wire 711 and second wire 712 may be a part of a conventional 2-wire, 4-wire cable, or a portion of a multi-pair cable.

Pick-off signal conditioning circuitry 720 receives input signals from first pick-off 605, second pick-off 605', and temperature sensor 607 via paths 611, 611' and 612. Pick-off circuitry 720 determines the frequency of the pick-off signals and may also determine properties of a material flowing through conduits 603A-603B. After the frequency of the input signals from pick-off sensors 605-605' and properties of the material are determined, parameter signals carrying this information are generated and transmitted to a secondary processing unit 750 in host system 700 via path 721. In a preferred embodiment, path 721 includes 2 leads. However, one skilled in the art will recognize that path 721 may be carried over first wire 711 and second wire 712 or over any other number of wires.

Host system 700 includes a power supply 730 and processing system 750. Power supply 730 receives electricity from a source and converts the received electricity to the proper power needed by the system. Processing system 750 receives the parameter signals from pick-off signal conditioning circuitry 720 and then may perform processes needed to provide properties of the material flowing through

conduits 603A-603B needed by a user. Such properties may include but are not limited to density, mass flow rate, and volumetric flow rate. Processing system 750 performs the processes shown in FIGS. 3 and 5 to provide a tamper prevention system in accordance with the present invention.

The above description provides an exemplary embodiment of the tampering prevention system in accordance with this invention. It is expected that those skilled in the art can and will design alternative embodiments that infringe on this invention as set forth in the claims below either literally or through the Doctrine of Equivalents.

What is claimed is:

1. A system for preventing tampering with signal conditioning circuitry in electronics that determines a parameter from signals received from sensors, said system comprising:

a host system that receives data from and send data to said signal conditioning circuitry;

a processing unit in said host system;

a memory connected to said processing unit;

instructions for directing said processing unit in said host system to periodically transmit a request for authentication information from said signal conditioning circuitry, receive said authentication information from said signal conditioning circuitry in response to said request, and store a record of said authentication information received from said signal conditioning circuitry in said memory; and

a media readable by said processing unit for storing said instructions.

2. The system of claim 1 wherein said authentication information includes a unique identification for said signal conditioning circuitry.

3. The system of claim 1 wherein said authentication information includes calibration data for said signal conditioning circuitry.

4. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to compare said authentication information with initial information, and signal an error in response to said authentication information not being equal to said initial information.

5. The system of claim 4 wherein said instruction for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to terminate operation of said system.

6. The system of claim 4 wherein said instructions include:

instructions for directing said processing unit to obtain said initial information.

7. The system of claim 6 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:

transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,

receive said authentication information from said signal conditioning circuitry, and

store said authentication information as said initial information in said memory.

8. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to compare said authentication information with initial information, and perform a programmed function in response to said authentication information not being equal to said initial information.

9. The system of claim 1 further comprising:

a processing unit in said signal conditioning circuitry;

a memory connected in said signal conditioning circuitry that stores said authentication information;

instructions for directing said processing unit in said signal conditioning circuitry to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioning circuitry for storing said instructions.

10. The system of claim 1 wherein said record includes a time stamp indicating when said authentication information is received.

11. The system of claim 1 wherein said record includes said authentication information received from said signal conditioning circuitry.

12. Meter electronics for a Coriolis flowmeter that detects possible tampering comprising:

a host system that receives parameter signals indicating properties of a material flowing through said Coriolis flowmeter from said signal conditioner and supplies powers to signal conditioner;

a signal conditioner remote from said host system and communicatively connected to said host system wherein said signal conditioner receives pick-off signals from sensors affixed to said Coriolis flowmeter and generates said parameter signals from said pick-off signals;

a processing unit in said host system;

a memory connected to said processing unit in said host system;

instructions for directing said processing unit in said host system to:

periodically transmit a request for authentication information to said signal conditioner,

receive said authentication information from said signal conditioner in response to said request, and

store said authentication information in said memory; and

a media readable by said processing unit for storing said instructions.

13. The meter electronics of claim 12 wherein said authentication information includes a unique identification for said signal conditioner.

14. The meter electronics of claim 12 wherein said authentication information includes calibration data for said signal conditioner.

15. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and

signal an error in response to said authentication information not being equal to said initial information.

16. The meter electronics of claim 15 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to terminate operation of said system.

17. The meter electronics of claim 16 wherein said instructions include:

instructions for directing said processing unit to obtain said initial information.

18. The meter electronics of claim 17 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:

transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,

receive said authentication information from said signal conditioning circuitry, and

store said authentication information as said initial information in said memory.

19. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and

perform a programed function in response to said authentication information not being equal to said initial information.

20. The meter electronics of claim 12 further comprising:

a processing unit in said signal conditioner;

a memory connected in said signal conditioner that stores said authentication information;

instructions for directing said processing unit in said signal conditioner to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioner for storing said instructions.

21. The meter electronics of claim 12 wherein said record includes a time stamp indicating when said authentication information is received.

22. The meter electronics of claim 12 wherein said record includes said authentication information received from said signal conditioner.

23. A Coriolis flowmeter having tamper resistant meter electronics comprising:

at least one flow tube through which material flows;

a driver affixed to said at least one flow tube that vibrates said at least one flow tube as said material flows through said at least one flow tube;

sensors affixed to at least two different points of said at least one flow tube to generate sensor signals indicating vibrations of said at least one flow tube at said at least two different points;

a signal conditioner that transmits a drive signal to said driver, receives said sensors signals, and generates parameter signals from said sensors signals wherein said parameter signals indicate a property of said material;

a host system that provides power to said signal conditioner and receives said parameter signals from said signal conditioner;

a processing unit in said host system;

a memory connected to said processing unit in said host system;

instructions for directing said processing unit in said host system to:

periodically transmit a request for authentication information to said signal conditioner,

receive said authentication information from said signal conditioner in

response to said request, and

store said authentication information in said memory; and

a media readable by said processing unit for storing said instructions.

24. The Coriolis flowmeter of claim 23 wherein said authentication information includes a unique identification for said signal conditioner.

25. The Coriolis flowmeter of claim 23 wherein said authentication information includes calibration data for said signal conditioner.

26. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and

signal an error in response to said authentication information not being equal to said initial information.

27. The Coriolis flowmeter of claim 26 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to terminate operation of said Coriolis flowmeter in response to said signal.

28. The Coriolis flowmeter of claim 26 wherein said instructions for directing said host system include:

instructions for directing said processing unit to obtain said initial information.

29. The Coriolis flowmeter of claim 28 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:

transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,

receive said authentication information from said signal conditioning

circuitry, and

store said authentication information as said initial information in said memory.

30. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and

perform a programmed function in response to said authentication information not being equal to said initial information.

31. The Coriolis flowmeter of claim 23 further comprising:

a processing unit in said signal conditioner;

a memory connected in said signal conditioner that stores said authentication information;

instructions for directing said processing unit in said signal conditioner to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioner for storing said instructions.

32. The Coriolis flowmeter of claim 23 wherein said record includes a time stamp indicating when said authentication information is received.

33. The Coriolis flowmeter of claim 23 wherein said record includes said authentication information received from said signal conditioner.

34. A method for preventing tampering with signal conditioning circuitry in a system comprising the steps of:

periodically transmitting a request for authentication information from a host system to said signal conditioner;

receiving said authentication information from said signal conditioning circuitry

in response to said request; and

storing said authentication information in a memory in said host system.

35. The method of claim 34 wherein said authentication information includes a unique identification for said signal conditioning circuitry.

36. The method of claim 34 wherein said authentication information includes calibration data for said signal conditioner.

37. The method of claim 34 further comprises the steps of:

comparing said authentication information with initial information stored in said host system; and

signaling an error in response to said authentication information not being equal to said initial information.

38. The method of claim 37 further comprises the steps of:

terminating operation of said system in response to said signal of said error.

39. The method of claim 38 further comprises the step of:

obtaining said initial information.

40. The method of claim 39 wherein said step of obtaining said initial information comprises the steps of:

transmitting a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system;

receiving said authentication information from said signal conditioning circuitry; and

storing said authentication information as said initial information in said memory.

41. The method of claim 34 further comprising the steps of:

receiving said request for said authentication information in said signal

conditioning circuitry;

reading said authentication information from a memory in said signal conditioning circuitry; and

transmitting said authentication information to said host system.

42. The method of claim 34 wherein said record includes a time stamp indicating when said authentication information is received.

43. The method of claim 34 further comprises the steps of:

comparing said authentication information with initial information stored in said host system; and

performing a programmed function in response to said authentication information not being equal to said initial information.

ABSTRACT

A system for prevention of tampering with signal conditioning circuitry. In accordance with this invention a host system remote from the signal conditioner periodically transmits a request for authentication information to the signal conditioner. The signal conditioning circuitry receives the request and transmits authentication information back to the host system. The host system receives the authentication information from the signal conditioning circuitry and stores the authentication information in memory to provide an audit trail.

DOCKET ALARM

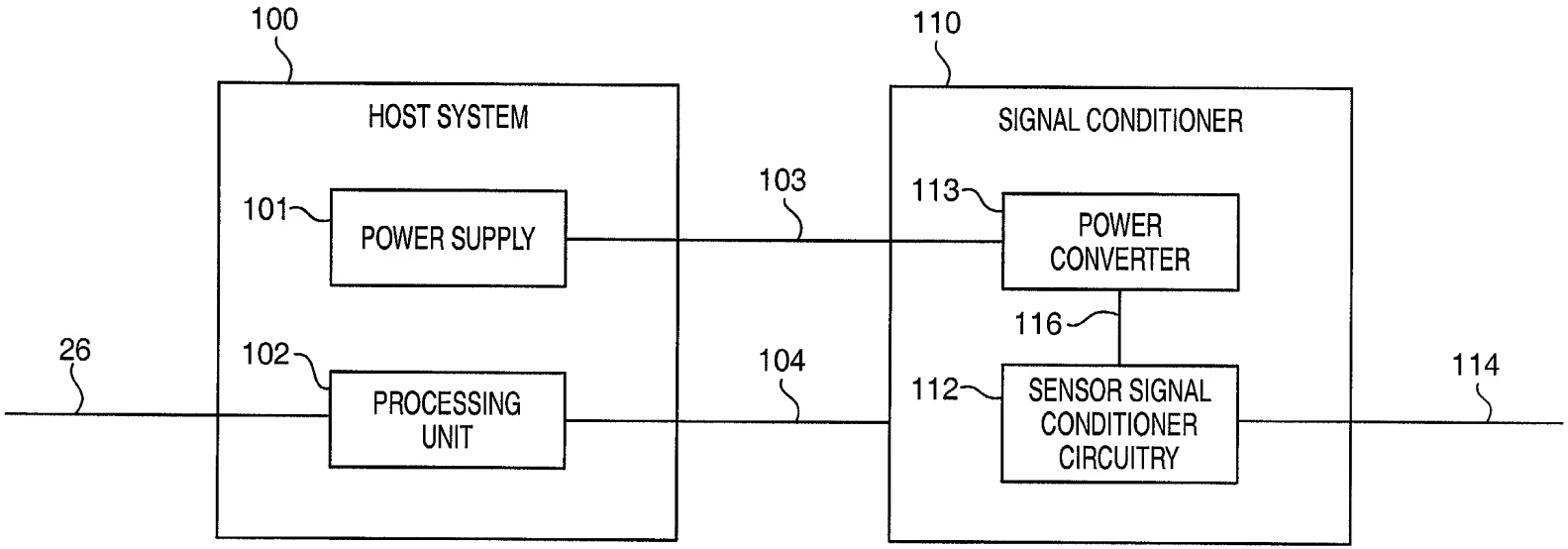


FIG. 1

Doc ID: US 2006/0181540 A1

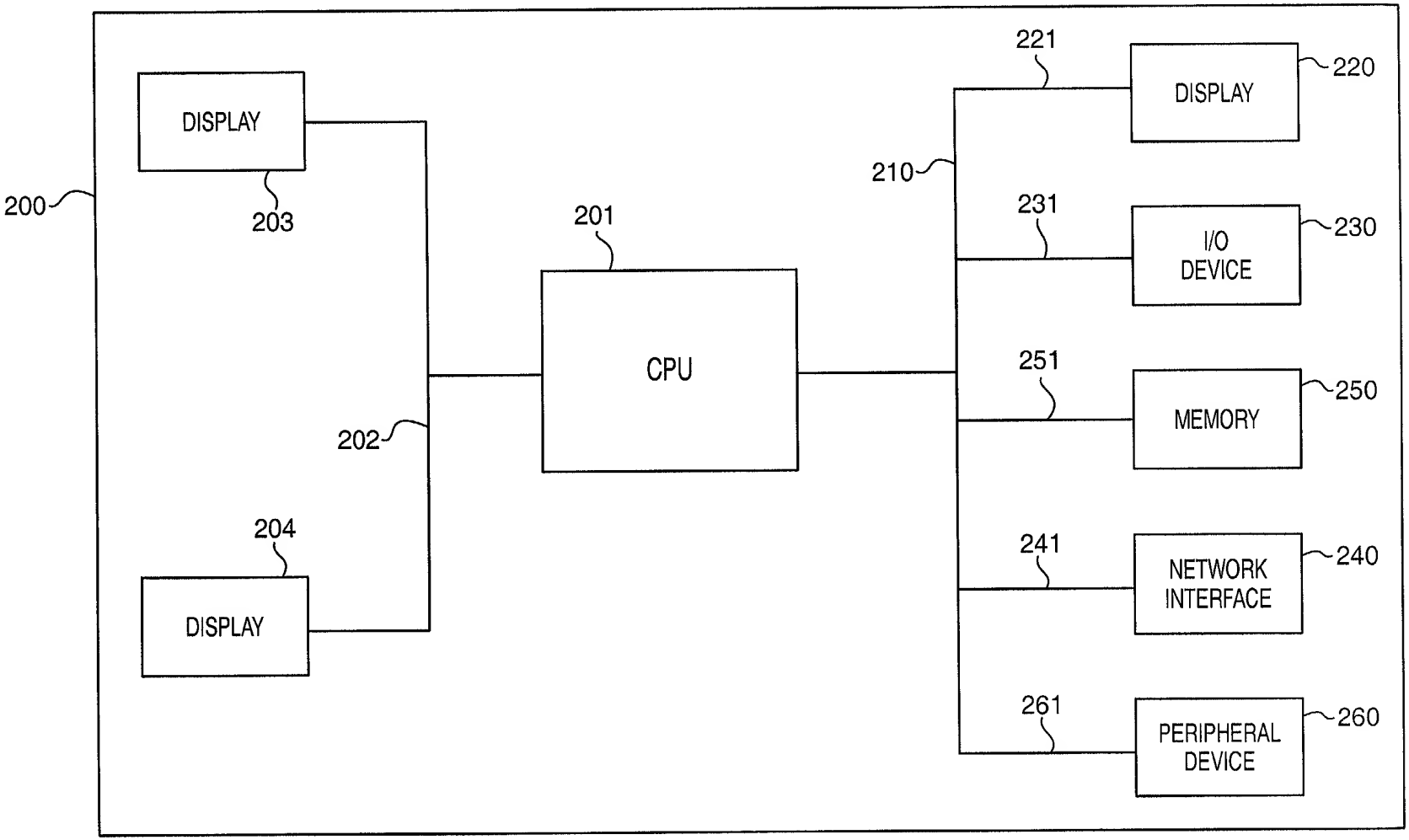


FIG. 2

FIG. 3

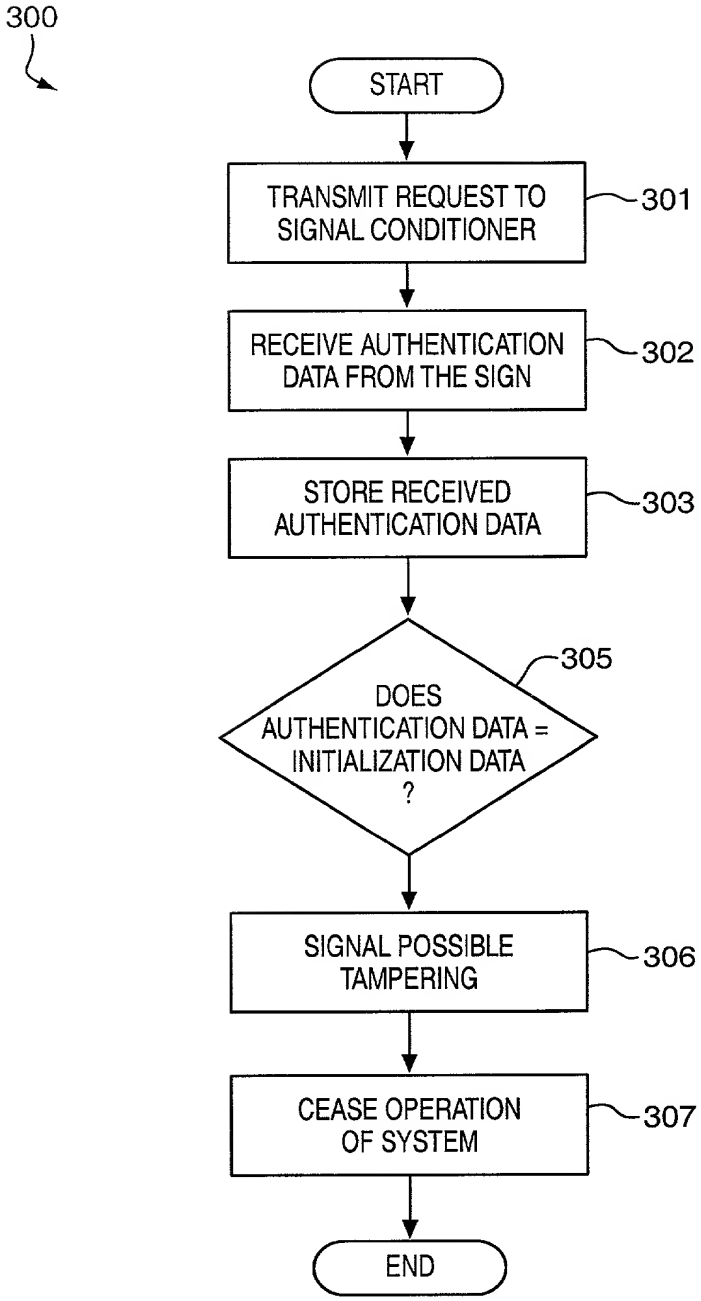

300
START
TRANSMIT REQUEST TO SIGNAL CONDITIONER
301
RECEIVE AUTHENTICATION DATA FROM THE SIGN
302
STORE RECEIVED AUTHENTICATION DATA
303
DOES AUTHENTICATION DATA = INITIALIZATION DATA ?
305
SIGNAL POSSIBLE TAMPERING
306
CEASE OPERATION OF SYSTEM
307
END

FIG. 4

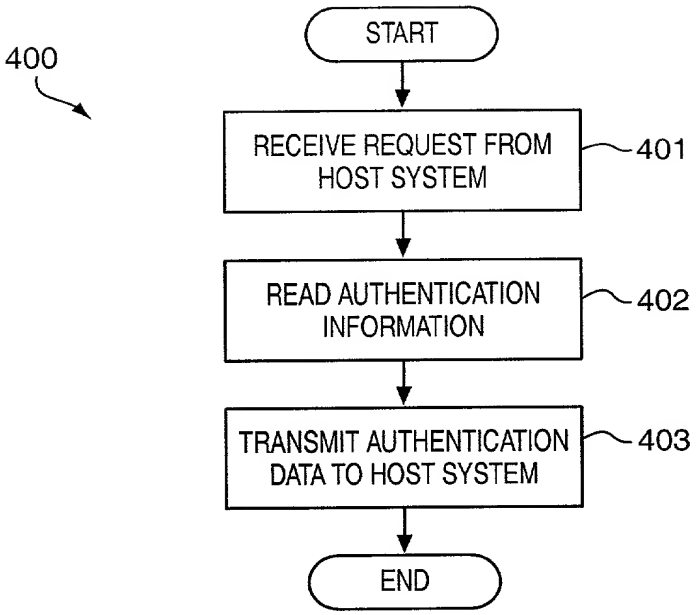
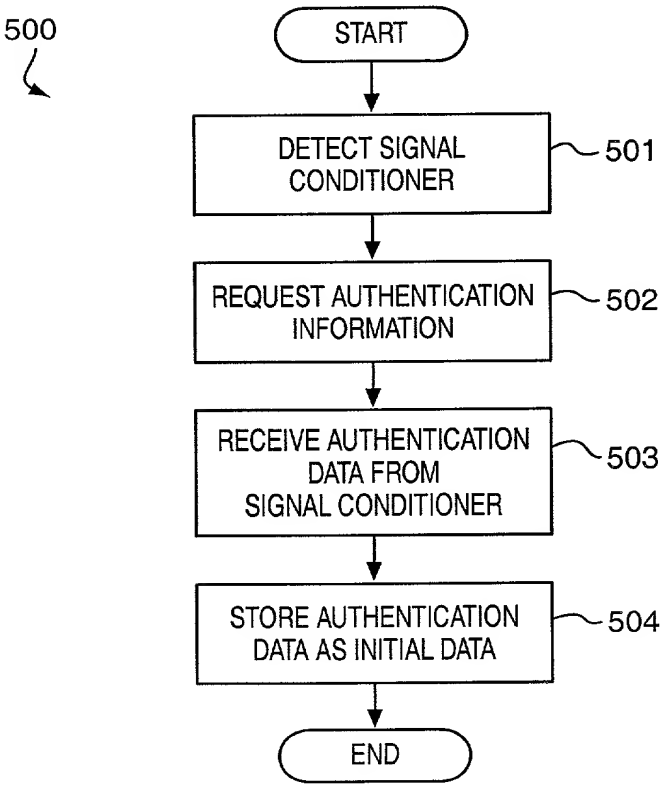

400
START
RECEIVE REQUEST FROM HOST SYSTEM
401
READ AUTHENTICATION INFORMATION
402
TRANSMIT AUTHENTICATION DATA TO HOST SYSTEM
403
END

FIG. 5


500
START
DETECT SIGNAL CONDITIONER
501
REQUEST AUTHENTICATION INFORMATION
502
RECEIVE AUTHENTICATION DATA FROM SIGNAL CONDITIONER
503
STORE AUTHENTICATION DATA AS INITIAL DATA
504
END

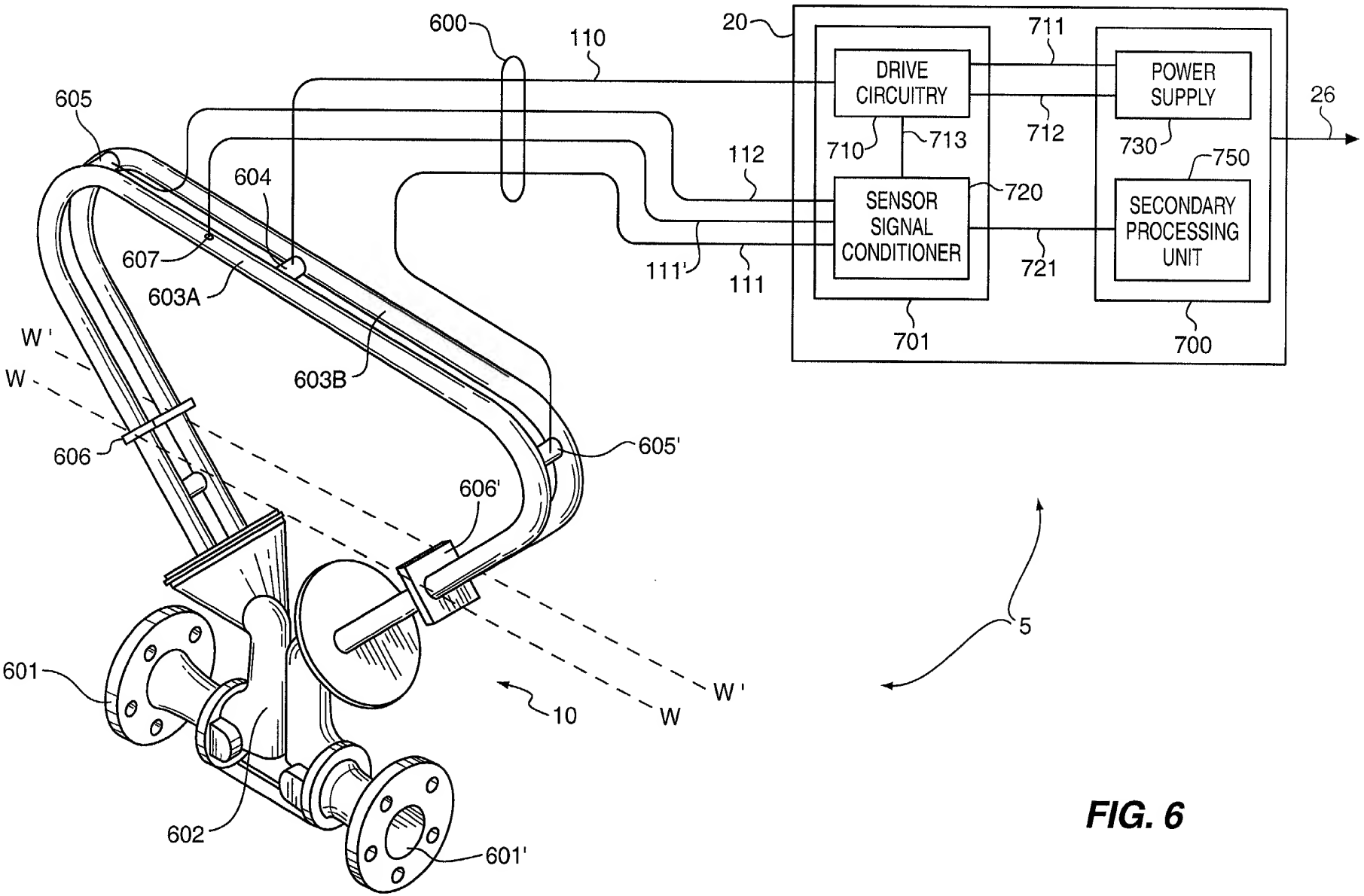

600
110
20
711
DRIVE CIRCUITRY
POWER SUPPLY
26
605
712
710
713
730
750
112
604
720
SENSOR SIGNAL CONDITIONER
SECONDARY PROCESSING UNIT
607
111'
111
721
603A
701
700
W'
W
603B
605'
606
606'
5
601
10
W'
W
602
601'

FIG. 6

Practitioner's Docket No. 5010/097 *PATENT*

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL, CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for an original application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor *(if only one name is listed below)* or an original, first and joint inventor *(if plural names are listed below)* of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

SYSTEM FOR PREVENTING TAMPERING WITH A SIGNAL CONDITIONER REMOTE FROM A HOST SYSTEM

SPECIFICATION IDENTIFICATION

The specification is attached hereto.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

William P. Wilbar	Registration Number 43,265
Dan Cleveland, Jr.	Registration Number 36,106
Donald M. Duft	Registration Number 17,484
Carl A. Forest	Registration Number 28,494
James M. Graziano	Registration Number 28,300
Michael J. Setter	Registration Number 37,936
Thomas Swenson	Registration Number 36,696
Curtis A. Vock	Registration Number 38,356
Travis C. Stephenson	Registration Number 45,132
Kirk D. Williams	Registration Number 42,229
Steven W. Weinrieb	Registration Number 26,520

SEND CORRESPONDENCE TO

William P. Wilbar
Duft, Graziano & Forest, P.C.
1790 - 30th Street, Suite 140
Boulder, CO 80301-1018 USA

DIRECT TELEPHONE CALLS TO:

William P. Wilbar
(303) 449-9497

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Allan L. Samson
Inventor's signature Allan L. Samson
Date 10-Jan. 2000 **Country of Citizenship** United States of America
Residence Fort Lupton, CO
Post Office Address 2643 County Road 19
Fort Lupton, CO 80621-8407

Michael Keilty
Inventor's signature Michael J. Keilty
Date 17-January 2000 **Country of Citizenship** United States of America
Residence Lyons, CO
Post Office Address 211 Pinewood Drive
Lyons, CO 80540-8130